Cryptography and Communications (2020) 12:769–784
https://doi.org/10.1007/s12095-019-00420-3

Double bordered constructions of self-dual codes from group rings over Frobenius rings

Joe Gildea[1] · Rhian Taylor[1] · Abidin Kaya[2] · A. Tylyshchak[3]

Received: 3 June 2019 / Accepted: 5 December 2019 / Published online: 9 January 2020

Abstract
In this work, we describe a double bordered construction of self-dual codes from group rings. We show that this construction is effective for groups of order $2p$ where p is odd, over the rings $\mathbb{F}_2 + u\mathbb{F}_2$ and $\mathbb{F}_4 + u\mathbb{F}_4$. We demonstrate the importance of this new construction by finding many new binary self-dual codes of lengths 64, 68 and 80; the new codes and their corresponding weight enumerators are listed in several tables.

Keywords Group rings · Self-dual codes · Codes over rings · Extremal codes · Bordered constructions

Mathematics Subject Classification (2010) 94B05 · 94B15

1 Introduction

Group rings and algebraic coding theory have been extensively studied as a result of their numerous theoretical and practical applications in cryptography, error correction and lattices to name a few. This strong connection between group rings and coding theory is frequently endorsed in the successful search for extremal binary self-dual codes. This has been an area of great research since the pure double-circulant construction was introduced in the 1960s [3, 24].

As the theory surrounding extremal binary self-dual codes is established, one remaining constraint is the size of the search field. A common technique in order to reduce the search field is to use special construction methods and apply certain restrictions; this frequently includes the use of group rings [23]. Fundamentally, Hurley [22] introduced a map from any

This research was supported by the London Mathematical Society (International Short Visits - Scheme 5).

✉ Rhian Taylor
rhian.taylor@chester.ac.uk

[1] Department of Mathematics, University of Chester, Chester, UK

[2] Sampoerna Academy, L'Avenue Campus 12780, Jakarta, Indonesia

[3] Department of Algebra, Uzhgorod National University, Uzhgorod, Ukraine

group ring element, to a matrix, A, over the ring of coefficients. The matrix, A, has been used in numerous construction methods to describe a linear code, [28]. This theory was well established with the realization of the [48,24,12] extended QR code as a group ring code for the dihedral group, [27]. Notably, in 1990 [1], the extended Golay codes were constructed from ideals in group rings. A popular technique, which has resulted in countless self-dual codes, has been to consider the generator matrix $(I_n|A)$ where A satisfies $AA^T = -I_n$, [18–20, 29, 30]. Initially applied over the binary field, these constructions can be extended over finite commutative rings. Recently, the theory surrounding group ring elements to construct codes has progressed to any group [9]. This has led to stronger connections between certain group ring elements called unitary units and self-dual codes [16].

The common double-circulant and four-circulant construction methods have been adjusted and modified numerous times in order to reduce the search field, in the hope of finding new extremal self-dual codes [8, 10, 17]. One particular modification of interest is the bordered double-circulant construction [2]. This construction method has shown considerable results, where the generator matrix is in the form:

$$\left[\begin{array}{c|c|ccc} & \alpha & \beta & \cdots & \beta \\ \hline & \beta & & & \\ I_n & \vdots & & A & \\ & \beta & & & \end{array}\right]$$

A natural extension of this work is to consider the following generator matrix where the identity matrix also has a border:

$$\left[\begin{array}{cc|ccccccc|cc|ccccccc} \alpha_1 & \alpha_2 & \alpha_3 & \cdots & \alpha_3 & \alpha_4 & \cdots & \alpha_4 & \alpha_5 & \alpha_6 & \alpha_7 & \cdots & \alpha_7 & \alpha_8 & \cdots & \alpha_8 \\ \alpha_2 & \alpha_1 & \alpha_4 & \cdots & \alpha_4 & \alpha_3 & \cdots & \alpha_3 & \alpha_6 & \alpha_5 & \alpha_8 & \cdots & \alpha_8 & \alpha_7 & \cdots & \alpha_7 \\ \hline \alpha_3 & \alpha_4 & & & & & & & \alpha_7 & \alpha_8 & & & & & & \\ \vdots & \vdots & & & & & & & \vdots & \vdots & & & & & & \\ \alpha_3 & \alpha_4 & & & & & & & \alpha_7 & \alpha_8 & & & & & & \\ \alpha_4 & \alpha_3 & & & & I_n & & & \alpha_8 & \alpha_7 & & & & A & & \\ \vdots & \vdots & & & & & & & \vdots & \vdots & & & & & & \\ \alpha_4 & \alpha_3 & & & & & & & \alpha_8 & \alpha_7 & & & & & & \end{array}\right]$$

Here, A is a matrix generated from a group ring element. In this paper, we put restrictions on the values of α and β in order to relax restrictions on the type of element chosen from the group ring.

This paper is organised as follows: Section 2 discusses the preliminaries, including definitions and notation, essential to the understanding and interpretation of results in this paper. In Section 3, we consider the new double bordered construction and look at the theory surrounding its effectiveness. We specify conditions on the construction in order to maximise its practicality and effectiveness. The following sections are allocated to the results, computed using MAGMA [25], and proving the efficiency of the theory. The new extremal binary self-dual codes are listed in numerous tables and summarised in the final section. Notably, this research includes new self-dual codes of length 64, 68 and 80.

2 Preliminaries

In this section, we will define extremal self-dual codes over Frobenius rings. We refer to certain types of these rings, of characteristic 2, throughout this paper. Here, we define the notation used in this paper in order to condense the results.

Frobenius rings can be characterised as follows. Denoting the character module of R by $\widehat{R}$, for a finite ring R the following are equivalent:

- R is a Frobenius ring.
- As a left module, $\widehat{R} \cong {}_R R$.
- As a right module, $\widehat{R} \cong R_R$.

The first commutative ring that we consider is $\mathbb{F}_2+u\mathbb{F}_2 := \mathbb{F}_2[X]/(X^2)$, where u satisfies $u^2 = 0$. The elements of the ring may be written as $0, 1, u$ and $1 + u$, where 1 and $1 + u$ are the units of $\mathbb{F}_2 + u\mathbb{F}_2$. We also consider $\mathbb{F}_4 + u\mathbb{F}_4$; the commutative binary ring of size 16. $\mathbb{F}_4 + u\mathbb{F}_4$ can be viewed as an extension of $\mathbb{F}_2 + u\mathbb{F}_2$. Therefore, we can express any element of $\mathbb{F}_4 + u\mathbb{F}_4$ in the form $\omega a + (1 + \omega)b$, where $a, b \in \mathbb{F}_2 + u\mathbb{F}_2$. These rings are generalised in [13] and [14]. In the upcoming results, we use the hexadecimal number system in order to represent the elements of $\mathbb{F}_4+u\mathbb{F}_4$. This is achieved by use of the ordered basis $\{u\omega, \omega, u, 1\}$.

$$\begin{aligned} 0 &\leftrightarrow 0000,\ 1 \leftrightarrow 0001,\ 2 \leftrightarrow 0010,\ 3 \leftrightarrow 0011,\\ 4 &\leftrightarrow 0100,\ 5 \leftrightarrow 0101,\ 6 \leftrightarrow 0110,\ 7 \leftrightarrow 0111,\\ 8 &\leftrightarrow 1000,\ 9 \leftrightarrow 1001,\ A \leftrightarrow 1010,\ B \leftrightarrow 1011,\\ C &\leftrightarrow 1100,\ D \leftrightarrow 1101,\ E \leftrightarrow 1110,\ F \leftrightarrow 1111. \end{aligned}$$

For example, the element $1 + u + u\omega$ in $\mathbb{F}_4 + u\mathbb{F}_4$ is expressed as 1011 from the ordered basis, which we refer to as B from the hexadecimal system.

Now, we will look at some definitions and notation regarding coding theory; the following is required for full understanding of the successive results. A code over a finite commutative ring R is defined as any subset C of R^n. An element of C is called a codeword. If a code satisfies $C = C^{\perp}$ then the code C is said to be self-dual, alternatively if $C \subseteq C^{\perp}$ then the code is said to be self-orthogonal. The Hamming weight enumerator of a code is defined as:

$$W_C(x, y) = \sum_{\mathbf{c} \in C} x^{n-wt(\mathbf{c})} y^{wt(\mathbf{c})}. \tag{1}$$

For binary codes, a self-dual code where all weights are congruent to 0 (mod 4) is said to be Type II and the code is said to be Type I otherwise. If a code satisfies $W_C(x, y) = W_{C^{\perp}}(x, y)$ then the code is said to be formally self-dual. The bounds on the minimum distances, $d(n)$ for Type I and Type II codes respectively, are

$$d(n) \leq 4\lfloor \frac{n}{24} \rfloor + 4$$

and

$$d(n) \leq \begin{cases} 4\lfloor \frac{n}{24} \rfloor + 4 \text{ if } n \not\equiv 22 \pmod{24} \\ 4\lfloor \frac{n}{24} \rfloor + 6 \text{ if } n \equiv 22 \pmod{24} \end{cases}$$

If these bounds are met for self-dual codes, they are called extremal. Extremal binary self-dual codes are of great interest for their numerous applications.

We also define the Gray maps ϕ' from $\mathbb{F}_2 + u\mathbb{F}_2$ to $\mathbb{F}_2^2$ given by $\phi'(a + bu) = (b, a + b)$ where $a, b \in \mathbb{F}_2$, and ϕ from $\mathbb{F}_4 + u\mathbb{F}_4$ to $\mathbb{F}_4^2$ given by $\phi(a + bu) = (b, a + b)$ where

$a, b \in \mathbb{F}_4$. Introduced in [7], ϕ is a distance preserving linear isometry which preserves orthogonality in the corresponding alphabets. We also consider the Gray maps ψ' from $\mathbb{F}_4$ to $\mathbb{F}_2^2$ given by $\psi'(a\omega + b\bar{\omega}) = (a, b)$ where $a, b \in \mathbb{F}_2$, and ψ from $\mathbb{F}_4 + u\mathbb{F}_4$ to $(\mathbb{F}_2 + u\mathbb{F}_2)^2$ given by $\psi(a\omega + b\bar{\omega}) = (a, b)$ where $a, b \in \mathbb{F}_4^2$. Initially introduced in [15], these maps were generalised in [26].

Next, we define a group ring and summarise its properties and notation; group rings are frequently used in various construction methods ([31]). Let G be a finite group or order n, then the group ring RG consists of $\sum_{i=1}^{n} \alpha_i g_i, \alpha_i \in R, g_i \in G$. Addition in the group ring is done by coordinate addition, namely

$$\sum_{i=1}^{n} \alpha_i g_i + \sum_{i=1}^{n} \beta_i g_i = \sum_{i=1}^{n} (\alpha_i + \beta_i) g_i. \tag{2}$$

The product of two elements in a group ring is given by

$$\left(\sum_{i=1}^{n} \alpha_i g_i \right) \left(\sum_{j=1}^{n} \beta_j g_j \right) = \sum_{i,j} \alpha_i \beta_j g_i g_j. \tag{3}$$

It follows that the coefficient of g_i in the product is $\sum_{g_i g_j = g_k} \alpha_i \beta_j$. Throughout this work, e_G denotes the identity element of any group G.

The following construction of a matrix was first given for codes over fields by Hurley in [22] and extended to rings in [9]. Let R be a finite commutative Frobenius ring and let $G = \{g_1, g_2, \ldots, g_n\}$ be the elements of a group of order n in a given listing. Let $v = \sum_{i=1}^{n} \alpha_{g_i} \in RG$. Define the matrix $\sigma(v) \in M_n(R)$ to be $\sigma(v) = (\alpha_{g_i^{-1} g_j})$ where $i, j \in \{1, 2, \cdots, n\}$.

Two groups that are often considered when applying the theory are cyclic and dihedral groups. For these groups, we consider circulant $n \times n$ matrices denoted $cir(\alpha_1, \alpha_2, \cdots, \alpha_n)$, where each row vector is rotated one element to the right relative to the preceding row vector [5]. Furthermore, the notation $CIR(A_1, A_2, \cdots, A_m)$ denotes the $nm \times nm$ circulant matrix constructed of m smaller $n \times n$ circulant matrices, A_i. We will now look at the structure of the matrix $\sigma(v)$ where v is an element of the cyclic or dihedral group of order $2p$.

Firstly, let $C'_{2p} = \langle x \mid x^{2p} = 1 \rangle$ and

$$v = \sum_{i=0}^{p-1} \sum_{j=0}^{1} \alpha_{i+pj+1} x^{2i+j} \in RC'_{2p}$$

then,

$$\sigma(v) = \begin{pmatrix} A_1 & A_2 \\ A'_2 & A_1 \end{pmatrix}$$

where $A_j = cir(\alpha_{(j-1)p+1}, \alpha_{(j-1)p+2}, \ldots, \alpha_{jp})$ and $A'_j = cir(\alpha_{jp}, \alpha_{(j-1)p+1}, \ldots, \alpha_{jp-1})$.

Alternatively, let $D_{2p} = \langle x, y \mid x^p = y^2 = 1, x^y = y^{-1} \rangle$ and

$$v = \sum_{i=0}^{p-1} \sum_{j=0}^{1} \alpha_{i+pj+1} x^i y^j \in RD_{2p}$$

then,

$$\sigma(v) = \begin{pmatrix} A_1 & A_2 \\ A_2^T & A_1^T \end{pmatrix}$$

where $A_j = cir(\alpha_{(j-1)p+1}, \alpha_{(j-1)p+2}, \ldots, \alpha_{jp})$.

We can use an effective technique in order to extend the length of a given code by 2. The following result, introduced in [12], will be utilised frequently in this work.

Theorem 2.1 *Let C be a self-dual code over $\mathbb{F}_2 + u\mathbb{F}_2$ of length n and $G = (r_i)$ be a $j \times n$ generator matrix for C, where r_i is the $i-$th row of G, $1 \leq i \leq k$. Let c be a unit in $\mathbb{F}_2 + u\mathbb{F}_2$ and X be a vector in $(\mathbb{F}_2 + u\mathbb{F}_2)^n$ with $\langle X, X\rangle = 1$ and $y_i = \langle r_i, X\rangle$. Then the following matrix*

$$\left(\begin{array}{cc|c} 1 & 0 & X \\ \hline y_1 & cy_1 & r_1 \\ \vdots & \vdots & \vdots \\ y_k & cy_k & r_k \end{array}\right)$$

generates a self-dual codes C' over $\mathbb{F}_2 + u\mathbb{F}_2$ of length $n + 2$.

3 Construction

Let $v \in RG$ where R is a finite Frobenius ring of characteristic 2 and G is a finite group of order $2p$ where p is odd. Define the following matrix:

$$M(\sigma) = \left[\begin{array}{cc|ccccccc|cc|ccccccc} \alpha_1 & \alpha_2 & \alpha_3 & \cdots & \alpha_3 & \alpha_4 & \cdots & \alpha_4 & \alpha_5 & \alpha_6 & \alpha_7 & \cdots & \alpha_7 & \alpha_8 & \cdots & \alpha_8 \\ \alpha_2 & \alpha_1 & \alpha_4 & \cdots & \alpha_4 & \alpha_3 & \cdots & \alpha_3 & \alpha_6 & \alpha_5 & \alpha_8 & \cdots & \alpha_8 & \alpha_7 & \cdots & \alpha_7 \\ \hline \alpha_3 & \alpha_4 & & & & & & & \alpha_7 & \alpha_8 & & & & & & \\ \vdots & \vdots & & & & & & & \vdots & \vdots & & & & & & \\ \alpha_3 & \alpha_4 & & & & & & & \alpha_7 & \alpha_8 & & & & & & \\ \alpha_4 & \alpha_3 & & & & I_{2p} & & & \alpha_8 & \alpha_7 & & & & \sigma(v) & & \\ \vdots & \vdots & & & & & & & \vdots & \vdots & & & & & & \\ \alpha_4 & \alpha_3 & & & & & & & \alpha_8 & \alpha_7 & & & & & & \end{array}\right]$$

where $\alpha_i \in R$. Let C_σ be a code that is generated by the matrix $M(\sigma)$. Then, the code C_σ has length $4p + 4$. Throughout this paper, we assume that G is a group of order $2p$ that contains a subgroup of order p where p is odd. If we fix a listing of G where the first p elements of G are the elements of H, then $\sigma(v)$ takes a certain form. The next result states the form that $\sigma(v)$ takes in this case. It also provides an important property that enables us to prove our main result.

Lemma 3.1 *Let R be a commutative ring. If $H = \{g_1, g_2, \ldots, g_p\}$ is a subgroup of the finite group $G = \{g_1, g_2, \ldots, g_p, g_{p+1}, \ldots, g_{2p}\}$ of order $2p$ (p is odd), then*

$$\sigma(v) = \left(\begin{array}{c|c} M_1 & M_2 \\ \hline M_2' & M_1' \end{array}\right),$$

where M_1, M_2 are $p \times p$ matrices, M_1' is permutation similar to M_1 and M_2' is permutation to M_2. Moreover

$$M_k \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix} = M_k^T \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix} = M_k' \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix} = {M_k'}^T \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix} = \begin{pmatrix} \mu_k \\ \vdots \\ \mu_k \end{pmatrix} (k = 1, 2),$$

where $\mu_1 = \sum_{g \in H} \alpha_g$, $\mu_2 = \sum_{g \in G \setminus H} \alpha_g$.

Proof Clearly, $M_1 = (\alpha_{g_i^{-1} g_j})_{i,j=1,\dots,p}$, $M_2 = (\alpha_{g_i^{-1} g_{p+j}})_{i,j=1,\dots,p}$ $M_2' = (\alpha_{g_{p+i}^{-1} g_j})_{i,j=1,\dots,p}$ and $M_1' = (\alpha_{g_{p+i}^{-1} g_{p+j}})_{i,j=1,\dots,p}$. Let $a \in G \setminus H$. Then, for any $1 \le i \le p$, $g_{p+i} \in aH$ and $g_{p+i} = a g_{\delta(i)}$ for some $1 \le \delta(i) \le p$. Moreover $\delta : i \to \delta(i)$ is a permutation of degree p and

$$M_1' = (\alpha_{g_{p+i}^{-1} g_{p+j}})_{i,j=1,\dots,p} = (\alpha_{(a g_{\delta(i)})^{-1} a g_{\delta(j)}})_{i,j=1,\dots,p} =$$

$$(\alpha_{g_{\delta(i)}^{-1} a^{-1} a g_{\delta(j)}})_{i,j=1,\dots,p} = (\alpha_{g_{\delta(i)}^{-1} g_{\delta(j)}})_{i,j=1,\dots,p}.$$

If we rearrange the rows and columns of the matrix $M_1 = (\alpha_{g_i^{-1} g_j})_{i,j=1,\dots,p}$ in the order $\delta(1), \dots \delta(p)$ we will obtain M_1'. So, M_1 is permutation similar to M_1'.

It is well known that group G of order $2p$ contains a subgroup of order 2. So there is $a \in G$ $a \ne e_G$, $a^2 = e_G$. Thus $|H| = p$, $a \notin H$. Again, let $g_{p+i} = a g_{\delta(i)}$ for some $1 \le \delta(i) \le p$. Moreover, $\delta : i \to \delta(i)$ is a permutation of degree p and

$$M_2 = (\alpha_{g_i^{-1} g_{p+j}})_{i,j=1,\dots,p} = (\alpha_{g_i^{-1} a g_{\delta(j)}})_{i,j=1,\dots,p},$$

$$M_2' = (\alpha_{g_{p+i}^{-1} g_j})_{i,j=1,\dots,p} = (\alpha_{(a g_{\delta(i)})^{-1} g_j})_{i,j=1,\dots,p} = (\alpha_{g_{\delta(i)}^{-1} a^{-1} g_j})_{i,j=1,\dots,p} = (\alpha_{g_{\delta(i)}^{-1} a g_j})_{i,j=1,\dots,p}.$$

Now, if we rearrange the rows of the matrix $M_2 = (\alpha_{g_i^{-1} a g_{\delta(j)}})_{i,j=1,\dots,p}$ in the order $\delta(1), \dots \delta(p)$ and if we rearrange the its columns in the order $\delta^{-1}(1), \dots \delta^{-1}(p)$ we will obtain

$$(\alpha_{g_{\delta(i)}^{-1} a g_{\delta(\delta^{-1}(j))}})_{i,j=1,\dots,p} = (\alpha_{g_{\delta(i)}^{-1} a g_j})_{i,j=1,\dots,p} = M_2'.$$

This implies that $S M_2 S = M_2'$ for a permutation matrix S, which contains ones in positions $(i, \delta(i))$ $(i = 1, \dots, p)$ or, which is the same, in positions $(\delta^{-1}(j), j)$ $(j = 1, \dots, p)$.

Now, the i-th element of column $M_1 \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix}$ is

$$\sum_{j=1}^{p} \alpha_{g_i^{-1} g_j} = \sum_{g \in H} \alpha_{g_i^{-1} g} = \sum_{g \in H} \alpha_g = \mu_1, \quad g_i \in H, \ g_i^{-1} \in H,$$

and the i-th element of column $M_1^T \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix}$ is

$$\sum_{j=1}^{p} \alpha_{g_j^{-1} g_i} = \sum_{g \in H} \alpha_{g^{-1} g_i} = \sum_{g \in H} \alpha_{g g_i} = \sum_{g \in H} \alpha_g = \mu_1, \quad g_i \in H.$$

Thus,

$$M_1\begin{pmatrix}1\\ \vdots\\ 1\end{pmatrix} = M_1^T\begin{pmatrix}1\\ \vdots\\ 1\end{pmatrix} = \begin{pmatrix}\mu_1\\ \vdots\\ \mu_1\end{pmatrix},$$

since we have $S\begin{pmatrix}1\\ \vdots\\ 1\end{pmatrix} = \begin{pmatrix}1\\ \vdots\\ 1\end{pmatrix}$ for any permutation matrix S, and M_1 is permutation similar to M_1'. Furthermore,

$$M_1'\begin{pmatrix}1\\ \vdots\\ 1\end{pmatrix} = {M_1'}^T\begin{pmatrix}1\\ \vdots\\ 1\end{pmatrix} = \begin{pmatrix}\mu_1\\ \vdots\\ \mu_1\end{pmatrix}.$$

Now, the i-th elements of columns $M_2\begin{pmatrix}1\\ \vdots\\ 1\end{pmatrix}$ and $M_2^T\begin{pmatrix}1\\ \vdots\\ 1\end{pmatrix}$ respectively, are

$$\sum_{j=1}^{p}\alpha_{g_i^{-1}g_{p+j}} = \sum_{g\in G\setminus H}\alpha_{g_i^{-1}g} = \sum_{g\in G\setminus H}\alpha_g = \mu_2,$$

$$\sum_{j=1}^{p}\alpha_{g_{p+j}^{-1}g_i} = \sum_{g\in G\setminus H}\alpha_{g^{-1}g_i} = \sum_{g\in G\setminus H}\alpha_{gg_i} = \sum_{g\in G\setminus H}\alpha_g = \mu_2,$$

where $g_i \in H$ and $g_i^{-1} \in H$.

Thus,

$$M_2\begin{pmatrix}1\\ \vdots\\ 1\end{pmatrix} = M_2^T\begin{pmatrix}1\\ \vdots\\ 1\end{pmatrix} = \begin{pmatrix}\mu_2\\ \vdots\\ \mu_2\end{pmatrix}$$

Therefore, we have $SM_1S = M_1'$ for some permutation matrix S, $S\begin{pmatrix}1\\ \vdots\\ 1\end{pmatrix} = \begin{pmatrix}1\\ \vdots\\ 1\end{pmatrix}$, and

$$M_2'\begin{pmatrix}1\\ \vdots\\ 1\end{pmatrix} = {M_2'}^T\begin{pmatrix}1\\ \vdots\\ 1\end{pmatrix} = \begin{pmatrix}\mu_2\\ \vdots\\ \mu_2\end{pmatrix}.$$

□

We can now state and prove our main result.

Theorem 3.2 *Let R be a finite commutative Frobenius ring of characteristic 2, $G = \{g_1, g_2, \ldots, g_p, g_{p+1}, \ldots, g_{2p}\}$ be a finite group of order $2p$ and $H = \{g_1, g_2, \ldots, g_p\}$ be a subgroup of group G. Then, C_σ is a self-dual code of length $4p+4$ if and only if*

- $\sum_{i=1}^{8}\alpha_i = 0$,
- $vv^* = 1 + \sum_{i=1}^{2}(\alpha_{i+2}^2 + \alpha_{i+6}^2)\widehat{g}$,
- $(\alpha_1+1)\alpha_3 + \alpha_2\alpha_4 + (\alpha_5+\mu_1)\alpha_7 + (\alpha_6+\mu_2)\alpha_8 = 0$,

- $(\alpha_1+1)\alpha_4+\alpha_2\alpha_3+(\alpha_5+\mu_1)\alpha_8+(\alpha_6+\mu_2)\alpha_7=0$ *and*
- $\begin{pmatrix} \alpha_1+\alpha_3^2+\alpha_4^2 & \alpha_2 & \alpha_5+\alpha_3\alpha_7+\alpha_4\alpha_8 & \alpha_6+\alpha_3\alpha_8+\alpha_4\alpha_7 & \alpha_7+\mu_1\alpha_3+\mu_2\alpha_4 & \alpha_8+\mu_1\alpha_4+\mu_2\alpha_3 \\ \alpha_2 & \alpha_1+\alpha_3^2+\alpha_4^2 & \alpha_6+\alpha_3\alpha_8+\alpha_4\alpha_7 & \alpha_5+\alpha_3\alpha_7+\alpha_4\alpha_8 & \alpha_8+\mu_1\alpha_4+\mu_2\alpha_3 & \alpha_7+\mu_1\alpha_3+\mu_2\alpha_4 \end{pmatrix}$
has free rank 2

where $\widehat{g}=\sum_{i=1}^{p}g_i$, $\mu_1=\sum_{g\in H}\alpha_g$ *and* $\mu_2=\sum_{g\in G\setminus H}\alpha_g$.

Proof Let $M(\sigma)=\begin{pmatrix} A_1 & A_2 & A_3 & A_4 \\ A_2^T & I_{2p} & A_4^T & \sigma(v) \end{pmatrix}$ where $A_1=\mathrm{circ}(\alpha_1,\alpha_2)$, $A_2=\mathrm{CIRC}(B_1,B_2)$, $A_3=\mathrm{circ}(\alpha_1,\alpha_2)$, $A_4=\mathrm{CIRC}(B_3,B_4)$, $B_1=(\alpha_3,\ldots,\alpha_3)\in R^p$, $B_2=(\alpha_4,\ldots,\alpha_4)\in R^p$, $B_3=(\alpha_7,\ldots,\alpha_7)\in R^p$ and $B_4=(\alpha_8,\ldots,\alpha_8)\in R^p$. Then

$$M(\sigma)M(\sigma)^T=\begin{pmatrix} A_1A_1^T+A_2A_2^T+A_3A_3^T+A_4A_4^T & A_1A_2+A_2+A_3A_4+A_4\sigma(v)^T \\ A_2^TA_1^T+A_2^T+A_4^TA_3^T+\sigma(v)A_4^T & A_2^TA_2+I_{2p}+A_4^TA_4+\sigma(v)\sigma(v)^T \end{pmatrix}.$$

Now,

$$A_1A_1^T+A_2A_2^T+A_3A_3^T+A_4A_4^T=\mathrm{circ}\left(\sum_{i=1}^{2}(\alpha_i^2+p\alpha_{i+2}^2+\alpha_{i+4}^2+p\alpha_{i+6}^2),0\right)=\mathrm{circ}\left(\sum_{i=1}^{8}\alpha_i^2,0\right)$$

and

$$A_2^TA_2+I_{2p}+A_4^TA_4+\sigma(v)\sigma(v)^T=\sum_{i=1}^{2}(\alpha_{i+2}^2+\alpha_{i+6}^2)\mathrm{CIRC}(\mathbf{A},\mathbf{0})+I_{2p}+\sigma(vv^*)$$

where $\mathbf{A}=\mathrm{circ}(\underbrace{1,\ldots,1}_{p-\text{times}})$ and $\mathbf{0}=\mathrm{circ}(\underbrace{0,\ldots,0}_{p-\text{times}})$. It follows from Lemma 3.1 that

$$\sigma(v)A_4^T=\begin{pmatrix} M_1 & M_2 \\ M_2' & M_1' \end{pmatrix}\begin{pmatrix} \alpha_7 & \alpha_8 \\ \vdots & \vdots \\ \alpha_7 & \alpha_8 \\ \alpha_8 & \alpha_7 \\ \vdots & \vdots \\ \alpha_8 & \alpha_7 \end{pmatrix}=\begin{pmatrix} \mu_1\alpha_7+\mu_2\alpha_8 & \mu_1\alpha_8+\mu_2\alpha_7 \\ \vdots & \vdots \\ \mu_1\alpha_7+\mu_2\alpha_8 & \mu_1\alpha_8+\mu_2\alpha_7 \\ \mu_1\alpha_8+\mu_2\alpha_7 & \mu_1\alpha_7+\mu_2\alpha_8 \\ \vdots & \vdots \\ \mu_1\alpha_8+\mu_2\alpha_7 & \mu_1\alpha_7+\mu_2\alpha_8 \end{pmatrix}=\mathrm{CIRC}((\mu_1\alpha_7+\mu_2\alpha_8)c,(\mu_1\alpha_8+\mu_2\alpha_7)c)$$

where $c=\begin{pmatrix}1\\ \vdots \\ 1\end{pmatrix}$. Additionally,

$$\begin{aligned} A_2^TA_1^T+A_2^T+A_4^TA_3^T+\sigma(v)A_4^T= &\ \mathrm{CIRC}((\alpha_1\alpha_3+\alpha_2\alpha_4)c,(\alpha_1\alpha_4+\alpha_2\alpha_3)c)+\mathrm{CIRC}(\alpha_3c,\alpha_4c) \\ &+\mathrm{CIRC}((\alpha_5\alpha_7+\alpha_6\alpha_8)c,(\alpha_5\alpha_8+\alpha_6\alpha_7)c) \\ &+\mathrm{CIRC}((\mu_1\alpha_7+\mu_2\alpha_8)c,(\mu_1\alpha_8+\mu_2\alpha_7)c) \end{aligned}$$

$$=\mathrm{CIRC}(\ ((\alpha_1+1)\alpha_3+\alpha_2\alpha_4+(\alpha_5+\mu_1)\alpha_7+(\alpha_6+\mu_2)\alpha_8)c,((\alpha_1+1)\alpha_4+\alpha_2\alpha_3+(\alpha_5+\mu_1)\alpha_8+(\alpha_6+\mu_2)\alpha_7)c)$$

.

Clearly, $M(\sigma)M(\sigma)^T$ is a symmetric matrix and C_σ is self orthogonal if $\sum_{i=1}^{8}\alpha_i^2=0$, $vv^*=1+\sum_{i=1}^{2}(\alpha_{i+2}^2+\alpha_{i+6}^2)\widehat{g}$,

$$\begin{aligned} (\alpha_1+1)\alpha_3+\alpha_2\alpha_4+(\alpha_5+\mu_1)\alpha_7+(\alpha_6+\mu_2)\alpha_8&=0 \text{ and} \\ (\alpha_1+1)\alpha_4+\alpha_2\alpha_3+(\alpha_5+\mu_1)\alpha_8+(\alpha_6+\mu_2)\alpha_7&=0. \end{aligned}$$

Moreover,

$$\operatorname{rank}(M(\sigma)) = \operatorname{rank}\left(\begin{array}{cc|ccc|cc|ccc} \alpha_1 & \alpha_2 & \alpha_3 & \cdots & \alpha_4 & \alpha_5 & \alpha_6 & \alpha_7 & \cdots & \alpha_8 \\ \alpha_2 & \alpha_1 & \alpha_4 & \cdots & \alpha_3 & \alpha_6 & \alpha_5 & \alpha_8 & \cdots & \alpha_7 \\ \hline \alpha_3 & \alpha_4 & & & & \alpha_7 & \alpha_8 & & & \\ \vdots & \vdots & & & & \vdots & \vdots & & & \\ \alpha_3 & \alpha_4 & & I_{2p} & & \alpha_7 & \alpha_8 & & \sigma(v) & \\ \alpha_4 & \alpha_3 & & & & \alpha_8 & \alpha_7 & & & \\ \vdots & \vdots & & & & \vdots & \vdots & & & \\ \alpha_4 & \alpha_3 & & & & \alpha_8 & \alpha_7 & & & \end{array}\right)$$

$$= \operatorname{rank}\left(\begin{array}{cc|ccc|cc|ccc} \alpha_1+\alpha_3^2 & \alpha_2+\alpha_3\alpha_4 & \alpha_3 & \cdots & \alpha_4 & \alpha_5+\alpha_3\alpha_7 & \alpha_6+\alpha_3\alpha_8 & \alpha_7 & \cdots & \alpha_8 \\ \alpha_2+\alpha_4\alpha_3 & \alpha_1+\alpha_4^2 & \alpha_4 & \cdots & \alpha_3 & \alpha_6+\alpha_4\alpha_7 & \alpha_5+\alpha_4\alpha_8 & \alpha_8 & \cdots & \alpha_7 \\ \hline 0 & c0 & & & & 0 & 0 & & & \\ \vdots & \vdots & & & & \vdots & \vdots & & & \\ 0 & 0 & & I_{2p} & & 0 & 0 & & \sigma(v) & \\ \alpha_4 & \alpha_3 & & & & \alpha_8 & \alpha_7 & & & \\ \vdots & \vdots & & & & \vdots & \vdots & & & \\ \alpha_4 & \alpha_3 & & & & \alpha_8 & \alpha_7 & & & \end{array}\right)$$

$$= \operatorname{rank}\left(\begin{array}{cc|ccc|cc|ccc} \alpha_1+\alpha_3^2+\alpha_4^2 & \alpha_2 & \alpha_3 & \cdots & \alpha_4 & \alpha_5+\alpha_3\alpha_7+\alpha_4\alpha_8 & \alpha_6+\alpha_3\alpha_8+\alpha_4\alpha_7 & \alpha_7 & \cdots & \alpha_8 \\ \alpha_2 & \alpha_1+\alpha_3^2+\alpha_4^2 & \alpha_4 & \cdots & \alpha_3 & \alpha_6+\alpha_3\alpha_8+\alpha_4\alpha_7 & \alpha_5+\alpha_3\alpha_7+\alpha_4\alpha_8 & \alpha_8 & \cdots & \alpha_7 \\ \hline 0 & 0 & & & & 0 & 0 & & & \\ \vdots & \vdots & & & & \vdots & \vdots & & & \\ 0 & 0 & & I_{2p} & & 0 & 0 & & \sigma(v) & \\ 0 & 0 & & & & 0 & 0 & & & \\ \vdots & \vdots & & & & \vdots & \vdots & & & \\ 0 & 0 & & & & 0 & 0 & & & \end{array}\right)$$

$$= \operatorname{rank}\left(\begin{array}{cc|ccc|cc|ccc} \alpha_1+\alpha_3^2+\alpha_4^2 & \alpha_2 & 0 & \cdots & \alpha_4 & \alpha_5+\alpha_3\alpha_7+\alpha_4\alpha_8 & \alpha_6+\alpha_3\alpha_8+\alpha_4\alpha_7 & \alpha_7+\mu_1\alpha_3 & \cdots & \alpha_8+\mu_2\alpha_3 \\ \alpha_2 & \alpha_1+\alpha_3^2+\alpha_4^2 & 0 & \cdots & \alpha_3 & \alpha_6+\alpha_3\alpha_8+\alpha_4\alpha_7 & \alpha_5+\alpha_3\alpha_7+\alpha_4\alpha_8 & \alpha_8+\mu_1\alpha_4 & \cdots & \alpha_7+\mu_2\alpha_4 \\ \hline 0 & 0 & & & & 0 & 0 & & & \\ \vdots & \vdots & & & & \vdots & \vdots & & & \\ 0 & 0 & & I_{2p} & & 0 & 0 & & \begin{array}{c|c} M_1 & M_2 \\ \hline M_2' & M_1' \end{array} & \\ 0 & 0 & & & & 0 & 0 & & & \\ \vdots & \vdots & & & & \vdots & \vdots & & & \\ 0 & 0 & & & & 0 & 0 & & & \end{array}\right)$$

$$= \operatorname{rank}\left(\begin{array}{cc|ccc|cc|ccc} \alpha_1+\alpha_3^2+\alpha_4^2 & \alpha_2 & 0 & \ldots & 0 & \alpha_5+\alpha_3\alpha_7+\alpha_4\alpha_8 & \alpha_6+\alpha_3\alpha_8+\alpha_4\alpha_7 & \gamma_1 & \cdots & \gamma_2 \\ \alpha_2 & \alpha_1+\alpha_3^2+\alpha_4^2 & 0 & \ldots & 0 & \alpha_6+\alpha_3\alpha_8+\alpha_4\alpha_7 & \alpha_5+\alpha_3\alpha_7+\alpha_4\alpha_8 & \gamma_2 & \cdots & \gamma_1 \\ \hline 0 & 0 & & & & 0 & 0 & & & \\ \vdots & \vdots & & & & \vdots & \vdots & & & \\ 0 & 0 & & I_{2p} & & 0 & 0 & & \begin{array}{c|c} M_1 & M_2 \\ \hline M_2' & M_1' \end{array} & \\ 0 & 0 & & & & 0 & 0 & & & \\ \vdots & \vdots & & & & \vdots & \vdots & & & \\ 0 & 0 & & & & 0 & 0 & & & \end{array}\right)$$

Table 1 Self-dual code of length 64 from D_6 over $\mathbb{F}_4 + u\mathbb{F}_4$

$\mathcal{A}_i$	$(\alpha_1, \ldots, \alpha_8)$	$(a_1, \ldots, a_6)$	$\lvert Aut(A_i)\rvert$	Type
1	$(0, B, 2, A, 2, 4, 1, 4)$	$(A, 1, 3, 2, B, 7)$	$2^3 \cdot 3$	$\beta = \mathbf{57}\ (W_{64,2})$
2	$(0, 1, 0, 0, 0, 2, 6, 7)$	$(0, B, B, 3, 6, 7)$	$2^4 \cdot 3$	$\beta = 64\ (W_{64,2})$

where $\gamma_1 = \alpha_7 + \mu_1\alpha_3 + \mu_2\alpha_4$ and $\gamma_2 = \alpha_8 + \mu_1\alpha_4 + \mu_2\alpha_3$. Therefore $M(\sigma)$ has free rank $2p + 2$ if and only if:

$$\begin{pmatrix} \alpha_1+\alpha_3^2+\alpha_4^2 & \alpha_2 & \alpha_5+\alpha_3\alpha_7+\alpha_4\alpha_8 & \alpha_6+\alpha_3\alpha_8+\alpha_4\alpha_7 & \alpha_7+\mu_1\alpha_3+\mu_2\alpha_4 & \alpha_8+\mu_1\alpha_4+\mu_2\alpha_3 \\ \alpha_2 & \alpha_1+\alpha_3^2+\alpha_4^2 & \alpha_6+\alpha_3\alpha_8+\alpha_4\alpha_7 & \alpha_5+\alpha_3\alpha_7+\alpha_4\alpha_8 & \alpha_8+\mu_1\alpha_4+\mu_2\alpha_3 & \alpha_7+\mu_1\alpha_3+\mu_2\alpha_4 \end{pmatrix}$$

has free rank 2. □

The next two results provide conditions when units/non units in RG can be used to be used to yield self-dual codes using the above construction.

Corollary 3.3 *Let R be a finite commutative Frobenius ring of characteristic 2, let G be a finite group of order $2p$ where p is odd, and let C_σ be a self-dual code. If $\sum_{i=1}^{2}(\alpha_{i+2} + \alpha_{i+6}) = 0$ then $v \in RG$ is a unit.*

Proof If $\sum_{i=1}^{2}(\alpha_{i+2} + \alpha_{i+6}) = 0$, then $\sigma(vv^*) = I_{2p}$ and $vv^* = 1$. Therefore v is unitary. □

Corollary 3.4 *Let R be a finite commutative Frobenius ring of characteristic 2, let G be a finite group of order $2p$ where p is odd, and let C_σ be a self-dual code. If $\sum_{i=1}^{2}(\alpha_{i+2} + \alpha_{i+6}) = 1$ then $v \in RG$ is a non-unit.*

Proof If $\sum_{i=1}^{2}(\alpha_{i+2} + \alpha_{i+6}) = 1$, then

$$\sum_{i=1}^{2}(\alpha_{i+2}^2 + \alpha_{i+6}^2)\mathrm{CIRC}(\mathbf{A}, \mathbf{0}) + I_{2p} + \sigma(vv^*) = \mathrm{CIRC}(\mathbf{A}, \mathbf{0}) + \sigma(vv^*) = 0$$

where $\mathbf{A} = \mathrm{circ}(0, \underbrace{1, \ldots, 1}_{(p-1)-\text{times}})$ and $\mathbf{0} = \mathrm{circ}(\underbrace{0, \ldots, 0}_{p-\text{times}})$. Now $det(\mathrm{CIRC}(\mathbf{A}, \mathbf{0})) = det(\mathbf{A})^2$ and

$$det(A) = det\begin{pmatrix} 0 & 1 & 1 & \ldots & 1 \\ 1 & 0 & 1 & \cdots & 1 \\ 1 & 1 & 0 & \cdots & 1 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & 1 & \ldots & 0 \end{pmatrix} = (p-1)det\begin{pmatrix} 1 & 1 & 1 & \ldots & 1 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & 1 \end{pmatrix} = 0.$$

Table 2 Self-dual codes of length 64 from D_{14} over $\mathbb{F}_2 + u\mathbb{F}_2$

$\mathcal{B}_i$	$(\alpha_1, \alpha_2, \ldots, \alpha_8)$	$(a_1, a_2, \ldots, a_{14})$	$\lvert Aut(C)\rvert$	Type
1	$(u, 1, u, u, 0, 0, u, 1)$	$(u, u, 0, u, u, 1, 1, 0, 0, 1, 3, 0, 3, 1)$	$2^3 \cdot 7$	$\beta = 46\ (W_{64,1})$
2	$(u, 1, u, u, 0, 0, u, 1)$	$(u, u, 0, 0, 0, 1, 1, u, 0, 1, 1, u, 1, 1)$	$2^2 \cdot 7$	$\beta = 60\ (W_{64,1})$

Table 3 Self-dual codes of length 64 from C'_{14} over R_1

$\mathcal{C}_i$	$(\alpha_1, \alpha_2, \ldots, \alpha_8)$	$(a_1, a_2, \ldots, a_{14})$	$\lvert Aut(C)\rvert$	Type
1	$(u, 1, u, u, 0, 0, u, 1)$	$(u, 0, 0, 0, u, 1, 1, 1, 0, 0, 1, 1, 0, 1)$	$2^3 \cdot 7$	$\beta = 46\ (W_{64,1})$

Therefore, $det(\sigma(vv^*)) = 0$ and vv^* is a non-unit by Corollary 3 in [22]. Hence, $v \in RG$ is a non-unit. □

4 Computational results

Now, we will construct self-dual codes of various lengths (64, 68, 80) using groups of order 6, 14, 18, 30 and 38.

4.1 Constructions coming from D_6

In this section, we implement the above construction using $G = D_6$. We construct self-dual codes of length 64 by considering this construction over $\mathbb{F}_4 + u\mathbb{F}_4$. Using this construction, we were able to construct one new code of length 64.

The possible weight enumerators for a self-dual Type I [64, 32, 12]-code is given in [4, 11] as:

$$W_{64,1} = 1 + (1312 + 16\beta)\, y^{12} + (22016 - 64\beta)\, y^{14} + \cdots, 14 \le \beta \le 284,$$
$$W_{64,2} = 1 + (1312 + 16\beta)\, y^{12} + (23040 - 64\beta)\, y^{14} + \cdots, 0 \le \beta \le 277.$$

With the most updated information, the existence of codes is known for β =14, 18, 22, 25, 29, 32, 35, 36, 39, 44, 46, 53, 59, 60, 64 and 74 in $W_{64,1}$ and for β =0, 1, 2, 4, 5, 6, 8, 9, 10, 12, 13, 14, 16, ..., 25, 28, 19, 30, 32, 33, 34, 36, 37, 38, 40, 41, 42, 44, 45, 48, 50, 51, 52, 56, 58, 64, 72, 80, 88, 96, 104, 108, 112, 114, 118, 120 and 184 in $W_{64,2}$.The new code that we have constructed is $\beta = 57$ in $W_{64,2}$.

4.2 Constructions coming from groups of order 14

Here we present the results for the above construction using $G \in \{D_{14}, C_{14}\}$. We construct self-dual codes of length 64 by considering this construction over $\mathbb{F}_2 + u\mathbb{F}_2$.

Table 4 Self-dual codes of length 80 from D_{18} over $\mathbb{F}_2 + u\mathbb{F}_2$ where $(\alpha_1, \ldots, \alpha_8) = (u, 1, u, u, 0, 0, u, 1)$

$\mathcal{D}_i$	$(a_1, \ldots, a_9)$	$(a_{10}, \ldots, a_{18})$	$\lvert Aut(C_i)\rvert$	Type
1	$(u, 0, u, 1, 1, 1, 1, 1, 1)$	$(u, u, 1, 3, 0, 1, 1, 1, 3)$	$2^2 \cdot 3^2$	$\alpha = \mathbf{-229}, \beta = \mathbf{18}\ (W_{80,2})$
2	$(u, u, u, 0, 1, u, 3, 3, 1)$	$(0, 0, 1, u, 3, u, 0, 3, 1)$	$2^2 \cdot 3^2$	$\alpha = \mathbf{-256}, \beta = \mathbf{18}\ (W_{80,2})$
3	$(0, u, 0, 0, u, 0, 0, 1, 1)$	$(0, 0, 1, 3, 1, 0, 3, 3, 3)$	$2^2 \cdot 3^2$	$\alpha = \mathbf{-274}, \beta = \mathbf{18}\ (W_{80,2})$
4	$(0, u, 0, 0, 0, 0, 0, 1, 3)$	$(u, 0, 1, 1, 1, 0, 3, 3, 3)$	$2^2 \cdot 3^2$	$\alpha = \mathbf{-310}, \beta = \mathbf{18}\ (W_{80,2})$
5	$(0, 0, 0, 1, 1, 3, 3, 3, 3)$	$(u, u, 1, 1, 0, 1, 3, 1, 3)$	$2^2 \cdot 3^2$	$\alpha = \mathbf{-355}, \beta = \mathbf{18}\ (W_{80,2})$

Table 5 Self-dual codes of length 80 from D_{38} over $\mathbb{F}_2$ where $(\alpha_1, \ldots, \alpha_8) = (0, 1, 0, 0, 1, 1, 0, 1)$

$\mathcal{E}_i$	$(a_1, \ldots, a_{19})$	$(a_{20}, \ldots, a_{38})$	$\lvert Aut(C_i)\rvert$	Type
1	(0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1)	(0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1)	$2 \cdot 19$	$\alpha = -\mathbf{211}, \beta = \mathbf{18}\ (W_{80,2})$
2	(0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1)	(0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1)	$2 \cdot 19$	$\alpha = -\mathbf{249}, \beta = \mathbf{18}\ (W_{80,2})$
3	(0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1)	(0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1)	$2 \cdot 19$	$\alpha = -\mathbf{287}, \beta = \mathbf{18}\ (W_{80,2})$
4	(0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1)	(0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1)	$2 \cdot 19$	$\alpha = -\mathbf{306}, \beta = \mathbf{18}\ (W_{80,2})$
5	(0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1)	(0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1)	$2^2 \cdot 19$	$\alpha = -\mathbf{325}, \beta = \mathbf{18}\ (W_{80,2})$
5	(0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1)	(0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1)	$2 \cdot 19$	$\alpha = -\mathbf{363}, \beta = \mathbf{18}\ (W_{80,2})$
7	(0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1)	(0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1)	$2^2 \cdot 19$	$\alpha = -\mathbf{401}, \beta = \mathbf{18}\ (W_{80,2})$

4.3 Constructions coming from a groups of order 18

Now, we implement the above construction using $G \in \{D_{18}, C_{18}\}$. We construct self-dual codes of length 80 by considering this construction over $\mathbb{F}_2 + u\mathbb{F}_2$. In [32], the possible weight enumerators for a self-dual Type I [80, 40, 14]-code is given in as:

$$W_{80,2} = 1 + (3200 + 4\alpha)\, y^{14} + (47645 - 8\alpha + 256\beta)\, y^{16} + \cdots,$$

where α and β are integers. A [80, 40, 14] was constructed in [6], however its weight enumerator was not stated. A [80, 40, 14] code was constructed in [21] with $\alpha = -280$, $\beta = 10$ and [80, 40, 14] codes were constructed for $\beta = 0$ and $\alpha = -17k$ where $k \in \{2, \ldots, 25, 27\}$ in [32]. None of the codes presented here have been previously constructed.

4.4 Constructions coming from D_{38}

In this section, we implement the construction on $G = D_{38}$. We construct self-dual codes of length 80 by considering this construction over $\mathbb{F}_2$.

5 New codes of length 68

In this section, we implement Theorem 2.1 to construct new extremal self-dual codes. We extend the codes previously constructed in Tables 1, 2 and 3.

The known weight enumerators of a self-dual $[68, 34, 12]_I$-code are as follows:

$$W_{68,1} = 1 + (442 + 4\beta)y^{12} + (10864 - 8\beta)y^{14} + \ldots$$
$$W_{68,2} = 1 + (442 + 4\beta)y^{12} + (14960 - 8\beta - 256\gamma)y^{14} + \ldots$$

where $0 \le \gamma \le 9$. Codes have been obtained for $W_{68,2}$ when

$\gamma = 2$, $\beta \in \{2m \,|m = 29, \ldots, 100, 103, 104\}$ or $\beta \in \{2m + 1 \,|m = 32, 34, \ldots, 79\}$;
$\gamma = 3$, $\beta \in \{2m \,|m = 40, \ldots, 98, 101, 102\}$ or
$\beta \in \{2m + 1 | m = 41, 43, \ldots, 77, 79, 80, 83, 96\}$;
$\gamma = 4$, $\beta \in \{2m \,|m = 43, 44, 48, \ldots, 92, 97, 98\}$ or
$\beta \in \{2m + 1 \,|m = 48, \ldots, 55, 58, 60, \ldots, 78, 80, 83, 84, 85\}$;
$\gamma = 5$ with $\beta \in \{m | m = 113, 116, \ldots, 181\}$;

Recall that the codes constructed in Tables 1, 2 and 3 are codes over $\mathbb{F}_4 + u\mathbb{F}_4$. Consequently, we converted these codes to codes over $\mathbb{F}_2 + u\mathbb{F}_2$ (using the Gray map $\psi_{\mathbb{F}_4+u\mathbb{F}_4}$)

Table 6 Self-dual codes of length 68 from extending $[64, 32, 12]_I$

$\mathcal{C}_{68,i}$	Code	c	X	γ	β
$\mathcal{C}_{68,1}$	$\mathcal{B}_1$	$u+1$	$(3, u, 0, u, 0, 3, u, u, 1, 0, u, 3, 0, 1, u, 1, 1, 1, u, u, u, u, 1, u, u, 0, 0, 1, u, 0, 3)$	**2**	**161**
$\mathcal{C}_{68,2}$	$\mathcal{B}_1$	$u+1$	$(u, 3, u, 3, u, 1, 0, 0, 1, 3, u, 0, u, u, 1, 0, 1, 3, 1, 0, 1, 3, u, 0, 3, 3, 0, 0, 0, u, 1, 3)$	**2**	**163**
$\mathcal{C}_{68,3}$	$\mathcal{A}_1$	1	$(0, 1, u, u, 1, 1, 3, u, 3, 1, 3, 0, 0, 0, 3, 1, 3, 0, 1, 0, 1, 1, u, u, 1, u, 3, 3, 0, 0, 3, u)$	**2**	**169**
$\mathcal{C}_{68,4}$	$\mathcal{B}_2$	$u+1$	$(0, u, 0, 1, 0, 0, 3, 0, 0, 0, 0, 3, 0, 0, 0, 1, 0, 1, u, 3, 1, 0, u, u, 3, 1, 1, 1, 1, 1, 0, u)$	**2**	**171**
$\mathcal{C}_{68,5}$	$\mathcal{C}_1$	$u+1$	$(1, 3, u, 0, 1, 3, 1, 3, 1, 0, 1, u, 0, 0, u, 3, 3, 0, u, 0, 3, u, 1, 0, 3, 1, 1, 0, u, 1, 1, u)$	**2**	**173**
$\mathcal{C}_{68,6}$	$\mathcal{A}_2$	1	$(3, 0, 0, 0, 3, 0, u, 3, 3, 3, u, 3, 0, 1, 1, 0, 3, u, 1, u, 0, 3, 0, u, u, 3, 0, 0, u, u, u, 1)$	**4**	**200**

Table 7 New codes of length 68 as neighbors of $\mathcal{C}_{68,6}$

$\mathcal{N}_{68,i}$	$(x_{35}, x_{36}, ..., x_{68})$	γ	β
$\mathcal{N}_{68,1}$	(11110001100011100000101111110001011)	**3**	**163**
$\mathcal{N}_{68,2}$	(10111000000000010111000000010011001)	**3**	**175**
$\mathcal{N}_{68,3}$	(00111000100011110011000000010110111)	**3**	**177**
$\mathcal{N}_{68,4}$	(10000100011010101110110011111101111)	**4**	**159**
$\mathcal{N}_{68,5}$	(10010001011000101111111100110010011)	**4**	**175**
$\mathcal{N}_{68,6}$	(11100011001101110100001110000010100)	**4**	**186**
$\mathcal{N}_{68,7}$	(11001011011001110100111011110111110)	**4**	**191**
$\mathcal{N}_{68,8}$	(11010011010111101001100010001101101)	**5**	**182**
$\mathcal{N}_{68,9}$	(10010010010111010111111011100001001)	**5**	**187**
$\mathcal{N}_{68,10}$	(00000001100001011011010011001000001)	**5**	**189**
$\mathcal{N}_{68,11}$	(01111001110110001100001110110101111)	**5**	**191**
$\mathcal{N}_{68,12}$	(00001011100011101011110101001111111)	**5**	**193**

before applying Theorem 2.1. The following table displays the newly constructed extremal codes of length 68. We replace $u + 1$ with 3 to save space (Tables 4 and 5).

Two self-dual binary codes of dimension k are said to be neighbors if their intersection has dimension $k - 1$. We consider the standard form of the generator matrix of C to reduce down the search field. Let $x \in \mathbb{F}_2^n - C$ then $D = \left\langle \langle x \rangle^{\perp} \cap C, x \right\rangle$ is a neighbor of C (Table 6). Without loss of generality, the first 34 entries of x are set to be 0, the rest of the vectors are listed in Table 7. As neighbors of codes in Table 5 we obtain 12 new codes with weight enumerators in $W_{68,2}$. All the codes have an automorphism group of order 2.

6 Conclusion

In this work, we have introduced a new construction for constructing self-dual codes using group rings. We provided certain conditions when this construction produces self-dual codes and we established a link between units/non-units and self-dual codes. We demonstrated the relevance of this new construction by constructing many binary self-dual codes, including new self-dual codes of length 64, 68 and 80.

- **Code of length 64:** We were to able to construct the following [64, 32, 12] codes with new weight enumerator in $W_{64,2}$:
$$\beta = \{57\}.$$
- **Codes of length 68:** We were able to construct the following extremal binary self-dual codes with new weight enumerators in $W_{68,2}$:
$$\begin{aligned} &(\gamma = 2, \quad \beta = \{161, 163, 169, 171, 173\}),\\ &(\gamma = 3, \quad \beta = \{163, 175, 177\}),\\ &(\gamma = 4, \quad \beta = \{159, 175, 186, 191, 200\}),\\ &(\gamma = 5, \quad \beta = \{182, 187, 189, 191, 193\}), \end{aligned}$$
- **Codes of length 80:** We were to able to construct the following [80, 40, 14] codes with new weight enumerators in $W_{80,2}$:
$$(\beta = 18, \quad \alpha = \{-211, -229, -249, -256, -274, -287, -306, -310, -325, -355, -363, -401\}).$$

References

1. Bernhardt, F., Landrock, P., Manz, O.: The extended Golay codes considered as ideals. J. Combin. Theory Ser. A **55**(2), 235–246 (1990)
2. Betsumiya, K., Georgiou, S., Gulliver, T.A., Harada, M., Koukouvinos, C.: On self-dual codes over some prime fields. Discrete Math. **262**(1–3), 37–58 (2003)
3. Chen, C.L., Peterson, W.W., Weldon, E.J.: Some results on quasi-cyclic codes. Inf. Control. **15**, 407–423 (1969)
4. Conway, J.H., Sloane, N.J.A.: A new upper bound on the minimal distance of self-dual codes. IEEE Trans. Inform. Theory **36**(6), 1319–1333 (1990)
5. Davis, P.J.: Circulant Matrices. Chelsea Publishing, New York (1979)
6. Dorfer, G., Maharaj, H.: Generalized AG codes and generalized duality. Finite Fields Appl. **9**, 194–210 (2018)
7. Dougherty, S.T., Gaborit, P., Harada, M., Sole, P.: Type II codes over $\mathbb{F}_2 + u\mathbb{F}_2$. IEEE Trans. Inform. Theory **45**, 32–45 (1999)
8. Dougherty, S.T., Gildea, J., Kaya, A.: Quadruple bordered constructions of self-dual codes from group rings. Cryptogr. Commun. https://doi.org/10.1007/s12095-019-00380-8 (2019)
9. Dougherty S.T., Gildea, J., Taylor, R., Tylshchak, A.: Group rings, G-codes and constructions of self-dual and formally self-dual codes. Des. Codes Cryptogr. **86**(9), 2115–2138 (2018)
10. Dougherty, S.T., Gildea, J., Korban, A., Kaya, A., Tylshchak, A., Yildiz, B.: Bordered constructions of self-dual codes from group rings and new extremal binary self-dual codes. Finite Fields Appl. **57**, 108–127 (2019)
11. Dougherty, S.T., Harada, M., Gulliver, T.A.: Extremal binary self-dual codes. IEEE Trans. Inform. Theory **43**(6), 2036–2047 (1997)
12. Dougherty, S.T., Kim, J.-L., Kulosman, H., Liu, H.: Self-dual codes over commutative Frobenius rings. Finite Fields Appl. **16**, 14–26 (2010)
13. Dougherty, S.T., Yildiz, B., Karadeniz, S.: Codes over R_k, gray maps and their binary images. Finite Fields Appl. **17**(3), 205–219 (2011)
14. Dougherty, S.T., Yildiz, B., Karadeniz, S.: Self-dual codes over R_k and binary self-dual codes. European J. Pure Appl. Math. **6**(1), 89–106 (2013)
15. Gaborit, P., Pless, V., Sole, P., Atkin, O.: Type II codes over $\mathbb{F}_4$. Finite Fields Appl. **8**(2), 171–183 (2002)
16. Gildea, J., Kaya, A., Taylor, R., Yildiz, B.: Constructions for self-dual codes induced from group rings. Finite Fields Appl. **51**, 71–92 (2018)
17. Gildea, J., Kaya, A., Yildiz, B.: An altered four circulant construction for self-dual codes from group rings and new extremal binary self-dual codes I. Discrete Math. **324**(12), 1–8 (2019)
18. Gulliver, T.A., Harada, M.: Weight enumerators of double circulant codes and new extremal self-dual codes. Des. Codes Cryptogr. **11**(2), 141–150 (1997)
19. Gulliver, T.A., Harada, M.: Classification of extremal double circulant formally self-dual even codes. Des. Codes Cryptogr. **11**(1), 25–35 (1997)
20. Gulliver, T.A., Harada, M.: On double circulant doubly even self-dual $[72, 36, 12]$ codes and their neighbors. Australas J. Combin. **40**, 137–144 (2008)
21. Gulliver, T.A., Harada, M.: Classification of extremal double circulant self-dual codes of lengths 74-88. Discr. Math. **306**, 2064–2072 (2006)
22. Hurley, T.: Group rings and rings of matrices. Int. J. Pure Appl. Math. **31**(3), 319–335 (2006)
23. Hurley, T.: Self-dual, dual-containing and related quantum codes from group rings. arXiv:0711.3983 (2007)
24. Karlin, M.: New binary coding results by circulants. IEEE Trans. Inform. Theory **15**, 81–92 (1969)
25. Bosma, W., Cannon, J.J., Fieker, C., Steel, A. (eds.): Handbook of Magma functions, Edition 2.16 (2010)

26. Ling, S., Sole, P.: Type II codes over $\mathbb{F}_4 + u\mathbb{F}_4$. Europ. J. Combinatorics **22**, 983–997 (2001)
27. Mcloughlin, I.: A group ring construction of the [48, 24, 12] Type II linear block code. Des. Codes Cryptogr. **63**(1), 29–41 (2012)
28. McLoughlin, I., Hurley, T.: A group ring construction of the extended binary Golay code. IEEE Trans. Inform. Theory **54**(9), 4381–4383 (2008)
29. Shi, M., Sok, L., Solé, P.: Self-dual codes and orthogonal matrices over large finite fields. Finite Fields and their Applications **54**, 297–314 (2018)
30. Shi, M., Qian, L., Solé, P.: On self-dual negacirculant codes of index two and four. Designs Codes and Cryptography **11**, 2485–2494 (2018)
31. Shi, M., Alahmadi, A., Solé, P.: Codes and rings: theory and practice. Academic Press, New York (2017)
32. Yankov, N., Anev, D., Gurel, M.: Self-dual codes with an automorphism of order 13. Adv. Math. Commun. **11**(3), 635–645 (2017)